REMARKS/ARGUMENTS

In view of both the amendments presented above and the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 USC § 103. Furthermore, the Applicants also submit that all of these claims now satisfy the requirements of 35 USC § 112. Thus, the Applicants believe that all of these claims are now in allowable form.

If the Examiner believes that there are any unresolved issues in any of the claims now pending in the application, the Examiner is urged to telephone Ms. Alberta A. Vitale, Esq. at (203) 469-8097 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Abstract and specification amendments

The Examiner objected to the abstract, as filed, owing to its inclusion, in line 5, of the term "said". The Applicants have now appropriately amended the abstract by deleting this term.

The Examiner also stated that "The specification has not been reviewed extensively for spelling and grammatical errors. It is requested that the Applicants do a thorough review of the document and fix any spelling or

grammatical errors." The Applicants have now carefully reviewed the specification and remedied various grammatical, idiosyncratic, spelling and typographical errors.

The Examiner also stated that "U.S. Patent Number 5,745,577 was cited as, 'US-A-5745577'. When a U.S. patent is cited for the first time it should be explicitly written as it appears above in order to avoid any confusion. Then any subsequent reference to the patent can be cited in an abbreviated fashion." Applicants have amended the specification so that the first occurrence of a reference to the U.S. Patent is in the required format.

The Examiner further referenced a citation at page 1, line 42 stating "it is unclear what the applicant is referring to." The citation has now been deleted.

Also, the Examiner noted that the sentence at page 2, line 42 of the specification is incomplete. In response, the Applicants have now amended their specification to include lines that were printed in the published application but had been inadvertently omitted from subsequently filed Amended Sheets. The Applicants have also slightly clarified the second line of the first full paragraph of text inserted on page 2 to specifically correct an idiomatic error by reciting "prior knowledge" instead of "being known".

To expedite entry of these amendments, the Applicants have enclosed a substitute specification.

None of the specification amendments adds any new matter to the specification and hence no new matter has been added to the substitute specification.

Claim Amendments

Claims 1, 2, 8, 10, 11, 14, 15, 16 and 22 have been amended. Claim 3 has been cancelled. Amended claims 2 represents a combination of the features of original claims 1-3.

New claims 26 through 32 have been added. Claims 26-30 are similar to claims 21-25. Claims 31 and 32 include limitations previously presented in claim 22.

Rejections under 35 U.S.C. § 112

The Examiner has implicitly rejected claim 1 under the provisions of 35 U.S.C. § 112 as being indefinite. Specifically, the Examiner stated "Claim 1 recites the limitation '...in order to mask the values (K; D) used in the process (P)' . . . There is insufficient antecedent basis for this limitation." The presently amended claim deletes reference to the value.

The Examiner has also rejected claims 8, 10, 11 and 14-16 under the provisions of 35 U.S.C. § 112 as being indefinite. In that regard, the Examiner states:

> Claims 8, 10, 11, 14-16 rejected . . . as being indefinite . . . . Claim 8 states the method consists of several steps, each step having one cryptographic function from the selection of F_i, F_i', $F_i"$. The dependent claims begin to select a specific function that could be different from the one previously chosen above. If F_i is chosen as the cryptographic function of claim 8, then a problem arises when claim 10 is reached and states; "Method according to claim 8, wherein the right-hand data (RD_i) is combined, in each step (S_i) and prior to the operation (F_i'), with the primary auxiliary value (A_i) of said step (S_i)." It is not clear if the applicant intends for the right-hand data to be combined before the specific operation of F_i' and only F_i', or if it should be assumed that whichever operation was chosen in claim 8 should be inserted instead.
>
> As it is currently stated in claim 10, it is assumed that the applicant is claiming a specific embodiment where the right-hand data (RD_i) is combined in each step (S_i) prior only to the operation (F_i'). The subsequent claims listed above induce the same confusion as claim 10 since the operation F;' and F; are used interchangeably.

In response, the Applicants have now appropriately amended claims 1, 8, 10, 11, and 14.

Further, the Examiner states that the word "preferably" in claim 22 renders the claim "indefinite". The Applicants have now amended claim 22 to simply delete the word "preferably".

Rejections under 35 U.S.C. § 102

The Examiner has rejected claims 1, 2, 7 and 8 under the provisions of 35 USC § 102 as being anticipated over the teachings in the Miyano patent (United States patent 5,442,705 issued to H. Miyano on August 15, 1995 (hereinafter Miyano)). This rejection is respectfully traversed.

In essence, the Miyano patent relates to "a hardware arrangement for transforming plaintext into corresponding ciphertext" (col. 1, lines 64-65) using multiple stages S_1-S_{16} (see Fig. 1 and col. 1, line 58). In each stage S_n, data R_n is ciphered by a cipher function F_n in dependence on a key K_n and then combined with data L_n, wherein the data L_n of computation stage n serves as data R_{n+1}, of computation stage n+1 and vice versa. (See col. 4, lines 5-21). "Suffix n denotes the n-th iteration." (Col. 3, line 21). The keys K_n for each "computation stage" (see Col. 2, line 62), S_n, are provided by a "key scheduling section 10" based on an "initial key". (See Col. 2, lines 65-66). In order to provide a computation that is "much more infeasible to be broken," the Miyano patent proposes use of a key that "is renewed at each iteration" (Col. 1, lines 12-13, emphasis added; and see Col. 5,

lines 38-42), which is accomplished in each stage S_n by a combination of an expanding permutation circuit E_n, an exclusive-or gate $EX\text{-}A_n$ and a memory M_n. Further embodiments (see Figs. 3-4) maintain the use of different keys in each iteration, but include additional memories MS1-3 to back-up the enciphering process in case of "bit errors during encipherment and/or during data transmission." (Col. 5, lines 65-66).

The Applicants respectfully request that the Examiner consider that in order to establish a prima facie case of anticipation, the Miyano patent must teach and every element of Applicants' claimed invention. As the Examiner will soon appreciate, the Miyano patent fails to do so.

A. Claim 1

The Applicants first address this rejection in the context of amended independent claim 1. Claim 1, recites:

> Method for cryptographically processing data, comprising:
> a) feeding, to a cryptographic process (P), values, namely, the data (X) and a key (K),
> b) carrying out the process (P) in order to form cryptographically processed output data (Y), characterized by
> c) feeding, to the process (P), <u>auxiliary values that mask the data (X) used in the process (P)</u>,

and

d) compensating, by an auxiliary process, the influence of the auxiliary values on the output data (Y). (Emphasis added).

The Examiner states that as per claim 1:

Miyano discloses a cryptographic system comprising: . . . Feeding, to a cryptographic process (P), values, namely the data (X) and a key (K), and carrying out the process (P) in order to form cryptographically processed output data (Y) (figure 1, where the Plaintext represents the data (X), Ciphertext represents the processed output (Y), Initial Key represents the key (K), and blocks Ro- R16 collectively represent the cryptographic process (P));

Characterized by feeding, to the process (P), auxiliary values (K*; A, B) and compensating, by an auxiliary process, the influence of the auxiliary values to the output data, in order to mask the values (K; D) used in the process (P) (figure 1, where K,- K16 represent auxiliary values, the Key Scheduling Section represents the auxiliary process).

Miyano does not mention the terms "compensating", "auxiliary" or "mask" in his invention. Unless applicant can further define these terms as they pertain to the invention, the key schedule compensates the influence of the auxiliary values K1-K16 by making the entire cryptographic process more secure. In addition, the key schedule masks the initial key. (Emphasis added).

The Applicants define the term "auxiliary value" in the specification at page 2, lines 17-19 as "a value [data

or key] which is fed to the process as a supplement to the corresponding data and key." According to the first embodiment of the present invention (see Fig. 2), an auxiliary value is also understood as a supplementary key (K*) from which the key (K) is generated by means of a supplementary process (P*). Assuming arguendo, that the initial key shown in Fig. 1 of the Miyano patent is interpreted as an "auxiliary value", then that initial key would be processed by the key scheduling section 10 to produce the keys K_1-K_{16} and thus masks the keys K_1-K_{16}. However, according to step c) of claim 1, the Applicants only require masking the data (X). This step limits the scope of independent claim 1 such that only the data, and not the key is masked by the auxiliary values. The Miyano patent, as explained above, only teaches the concept of masking the keys K_1-K_{16} (by the initial key) but not the data. Therefore, this patent does not disclose step c) of claim 1. Consequently, the key scheduling section 10 of the Miyano patent, which only impacts the initial key and the keys K_1-K_{16}, does not compensate the patent data for the influence of the auxiliary values (that mask the data only), in sharp contrast to that recited in step d) of Applicants' claim 1.

Accordingly, the Miyano patent does not disclose each and every step of independent claim 1, as amended and thus fails to anticipate claim 1, as it stands.

B. Claim 2

As to independent claim 2, this claim, as it now stands amended, recites:

> Method for cryptographically processing data, comprising;
> a) feeding, to a cryptographic process (P), values, namely data (X) and a key (K),
> b) carrying out the process (P) in order to form cryptographically processed output data (Y), characterized by
> c) feeding, to a supplementary process (P*), a supplementary key (K*) in order to form the key (K),
> d) wherein the supplementary key (K*) masks the key (K) used in the process (P), and
> e) wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed. (Emphasis added).

With respect to this claim, the Examiner states:

> An auxiliary value comprises a supplementary key (K*) which is fed to a supplementary process (P*) in order to form the key (K) (column 2, lines 65-66 ["A key scheduling section 10 is supplied with a 64-bit initial key including 8 parity bits."]; column 3, lines 47-49 ["The 16 keys K.sub.1 -K.sub.16 thus obtained are respectively applied to the stages S1-S16 and stored in corresponding memories M1-M16."], figure 1). Miyano does not mention the term "supplementary" in his invention but supplementary is defined as something added to complete a thing, make up for a

> deficiency, or extend or strengthen the whole. Since the key schedule strengthens the security of the system as a whole it is considered a supplementary process, while a key is fed to the key schedule and the keys, K_1- K16 are produced which act as auxiliary values to the primary process. (Emphasis added).

Step e) of this claim expressly recites that "the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed". Thus, this recitation clearly distinguishes supplementary process (P*) from the key scheduling section 10 of Fig. 1 of the Miyano patent which does not so utilize such an auxiliary key. Therefore, the Miyano patent does not disclose each and every step of independent claim 2, as amended, and hence fails to anticipate this claim.

C. Claim 7

Claim 7 recites:

> Method according to claim 2, wherein the process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary process (P*) are alternated.

The Examiner states:

> The process (P) and the supplementary process (P*) each are built up from a number of steps, and wherein steps of the process (P) and the supplementary

> process (P*) are alternated (column 1, lines 64-68; column 2, lines 1-2; figure 1). The process (P) is represented by the steps R_0- R_{16} and alternate with the key schedule process which represents (P*). The two processes alternate since a new auxiliary key must be produced by the key schedule before the next R; is executed.

Inasmuch as claim 7 depends from independent claim 1, claim 7 is not anticipated by the Miyano patent for the exact same reasons set forth above with respect to claim 1.

D. Claim 20

As to this claim, the Examiner states:

> According to the method of claim 8, combining is carried out using an XOR operation (Figure 3, column 4, lines 6-9). It can be seen in figure 3 that, as stated in claim 8, the right-handed data, R_n goes through the cipher function and then that processed data goes to the combinatory XOR operation EX_n' which also takes the left-handed data, L_n as its other input. (Emphasis added).

The rejection of claim 20 (which depends from claim 8) is baseless because the Miyano patent only discloses the use of an XOR operation, and not all other features of claim 8. For instance, this patent does not disclose the Applicants' claimed "the right-hand data (RD_1) is combined with a primary auxiliary value (A_1) prior to the first step (S_1)." (Claim 8, emphasis added). The initial

permutation 12 in Fig. 1 of this patent does not involve any auxiliary values at all. Therefore, claim 20 is not disclosed or taught by the Miyano patent, and hence not anticipated by it.

E. Claim 22

The Examiner also rejected claim 22 as being anticipated by the Miyano patent. Claim 22 depends from independent claim 1. Given that, the Applicants submit that claim 22 is not anticipated by the teachings of this patent for the exact same reasons set forth above regarding claim 1.

Rejections under 35 U.S.C. § 103

1. Miyano in view of Schneier

The Examiner has rejected claim 5 under the provisions of 35 USC § 103 as being obvious over the teachings in the Miyano patent taken in view of the Schneier publication (B. Schneier titled Applied Cryptography, ©1996, various pages). This rejection is respectfully traversed.

The Schneier reference focuses on the technique of "whitening," wherein key material is combined by means of an XOR operation with input data of a block algorithm, and other key material is combined by means of an XOR operation with output data of the block algorithm. This technique prevents

a cryptanalyst from obtaining a pair of plaintext and ciphertext that could be used to analyze the underlying enciphering algorithm. (See pages 363; and pages 366-67).

a. Claim 5

Claim 5 recites: "Method according to claim 2, wherein the data (X) is also fed to the supplementary process (P*)". With respect to this claim, the Examiner states:

> Miyano fails to teach the data (X) being fed to the supplementary process (P*) in addition to the auxiliary key (K*). However, Schneier discloses a process called whitening where the supplementary process is an XOR combinatory process and both the data and some key material are fed to the XOR process before executing the primary process, in this case, DES (Schneier, 15.6).
>
> It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to feed the data and the key to a supplementary XOR process in order to hide plaintext patterns, which is similar to masking, as stated in Schneier (pg 363). (Emphasis added).

Since claim 5 depends directly from independent claim 2, to facilitate prosecution, the Applicants will address the rejection in the context of the amended independent claim 2.

The "whitening" disclosed by the Schneier patent is not the same as features c), d) and e) of the independent

claim 2. Schneier describes "whitening" as "the technique of XORing some key material with the input to a block algorithm, and XORing some other key material with the output." (Schneier 15.6, p. 366). "The idea is to prevent a cryptanalyst from obtaining a plaintext/ciphertext pair for the underlying algorithm." Clearly this is not the same as Applicants "c) feeding . . . a supplementary key (K*) in order to form the key (K) . . . d) where the supplementary key (K*) masks the key (K) used in the process (P), and e) wherein the supplementary process (P*) comprises a cryptographic process to which an auxiliary key (K') is fed." Hence Schneier does not teach or disclose these features of Applicants claim. Since neither the Schneier reference nor the Miyano patent, alone or in combination, provide any teaching or suggestion of Applicants' claimed invention, claims 2 (steps c) d) and e) and 3) and claim 5 "supplementary process (P*)" cannot be rendered obvious by the teachings of these references taken singularly or in combination.

2. Miyano in view of Rivest

The Examiner has rejected claim 8 under the provisions of 35 USC § 103 as being obvious over the teachings in the Miyano patent taken in view of the Rivest patent (United States patent 5,724,705 issued to R. L. Rivest on March 3, 1998. This rejection is respectfully traversed.

The Rivest patent relates to "cipher methods and devices, and in particular to block-cipher cryptographic methods and devices." (Col. 1, lines 6-7). "A novel feature of the [presented] cipher is its heavy use of data-dependent rotations . . . which operate such that one word of intermediate results is cyclically rotated by an amount determined, for example, by some low-order bits of another word of the intermediate results. The data-dependent rotations in the cipher should frustrate differential cryptanalysis and linear cryptanalysis, which are two powerful techniques for cryptanalyzing block ciphers." (Col. 1, lines 59-67). The basic set-up of the cipher is depicted in Fig. 1B (see Col. 5, line 65 to col. 6, line 49), "wherein a plaintext input block 30 is stored in two . . . registers . . . 32 and . . . 34." (Col. 5, line 66-67). "An expanded key table [S 14] . . . is stored in a memory of the encryption device . . . [and] [s]ome of the expanded key table S 14 is initially added to the plaintext" (col. 6, lines 13-15) A, B (steps 40 and 42). (See, Col. 6, lines 21-36). In repeatedly performed steps 56 and 58, the plaintext A, B then is encrypted by XOR operations (steps 44, 46), left or right shifting operations (steps 48, 50) and additions of elements of the key table 14 (steps 52, 54). (See, Col. 6, lines 21-46). "The encrypted data output A(encrypt) 55 and B(encrypt) 57 then are <u>stored</u> in memory registers A and B, respectively." (Col. 6, lines 46-49, emphasis added).

a. Claim 8

Claim 8, as amended, recites:

> Method according to claim 1, wherein the process (P) comprises a number of steps (S_i), each having a cryptographic operation for processing right-hand data (RD_i) derived from the data (X) and a combinatory operation (C_i) for combining with left-hand data (LD_i) also derived from the data (X), the processed right-hand data (FD_i) in order to form modified left data (SD_i),and wherein the right-hand data (RD_i) is combined with a primary auxiliary value (A_1) prior to the first step(S_1) and the left-hand data(LD_1) is combined with an additional auxiliary value (A_0).

The Applicants' invention sets out from (public) cryptographic processes such as DES or RSA. Targeting to increase the resistance of these algorithms against cryptanalysis that is based on knowledge of the cryptographic process, the Applicants' mask the "data" (claim 1). The Rivest patent does not disclose any auxiliary values that are at least indirectly fed to the process (P) and that mask the data (X). The only values fed to the process taught by this patent are the elements of the key table S 14, and the plaintext 30. Consequently, due to the lack of auxiliary values, no masking of the data (X) can be accomplished. Furthermore, there is no auxiliary process that suppresses the influence of the (non-existent) auxiliary values on the output data (Y).

Additionally claim 1 recites that (a) auxiliary values are added to the process that masks the data (X) used in the process (P), and (b) the output data is compensated for any influence of the auxiliary values. No prior art has been identified that discloses or renders such an approach for masking data obvious. The Applicants' approach is particularly advantageous because the presence of the auxiliary values is not visible to an attacker, because it does not influence the result of the encryption. However, by using, in the steps of the encryption, masked data instead of the original input data (X), cryptanalysis is vastly aggravated particularly should the attacker assumes use of a known encryption process and the application of unmasked input data.

Concerning the Examiner's objections regarding claim 8 the values S[0] and S[1] that are added in the Rivest patent's encryption algorithm in steps 40 and 42 actually represent the encryption key, and not "auxiliary values" in the sense of the present application. Furthermore, the influence of these auxiliary values on the output data is not compensated by an auxiliary process, because then no encryption would have taken place at all.

For these reasons the Rivest patent, alone or in combination with the Miyano patent, fails to provide any teaching or suggestion of features c) and d) of claim 1. Hence these references fail to render claims 1 or 8 obvious.

3. Miyano in view of Bouricius

The Examiner has rejected claims 21, 23, 24 and 25 under the provisions of 35 U.S.C. § 103 as being obvious over the teachings in the Miyano patent taken in view of the Bouricius patent (United States patent 4,302,810 issued to W. G. Bouricius on November 24, 1981). For the sake of prosecution efficiency the rejection will be discussed in the context of claims 21, 23, 24 and 25 as well as newly added claims 26, 28, 29 and 30. This rejection is respectfully traversed.

The Bouricius patent relates to a method and apparatus "for use in an electronic funds transfer system wherein it is required that a Host (H) be reasonably guaranteed that a Person (P) and a Retailer (R) agree on the transaction details before the funds transfer takes place" (Claim 10, Col. 12, lines 3-7; and see claim 12 and Fig. 1). Therein, "a terminal under control of R [comprises] . . . a key-controlled block cipher encryption unit . . . for encrypting transaction messages to be sent to H,. . . and a portable transaction terminal device . . . under control of P [comprises] . . . a key-controlled block-cipher cryptographic unit . . . compatible with that in R's terminal." (Claim 10, Col. 12, lines 9-31). The portable transaction terminal device may comprise "a first unit including display means, a keyboard means, . . . arithmetic and logic circuitry and required storage registers for performing predetermined arithmetic operations on data entered into said device, and a second unit physically associatable with said first unit in

data exchange relationship therewith comprising a data storage and transfer card containing storage means for storing a personal data unique to P . . . and part or all of P's unique encryption key." (Claim 12, Col. 13, line 11 to Col. 14, line 11).

a. Claims 21, 23, 25, 26, 28 and 30

Each of claims 21, 23, and 25 depends either directly or indirectly, from independent claim 1. For the reasons given above with respect to the rejection of claim 1, claims 21, 23 and 25 are not rendered obvious by the teachings of the Miyano patent in view of those in the Bouricius patent. Furthermore, since the latter patent does not provide any teaching or suggestion of the encryption of transfer messages, it does not provide any teaching or suggestion of recitations a) and b) of claim 1.

Each of claims 26, 28 and 30 depends from independent claim 2. For the reasons given above with respect to the rejection of claim 2, claims 26, 28 and 30 are not rendered obvious by the teachings of the Miyano patent in view of those in the Bouricius patent. Additionally, the Bouricius patent does not provide any teaching or suggestion of the encryption of transfer messages, nor does it does not provide any teaching or suggestion of recitations a) and b) of claim 2. For all of these reasons, claims 26, 28 and 30 are not made obvious by the teachings of in either of these cited patents.

b. Claims 24 and 29

Claims 24 and 29, which depend from claims 23 and 28, respectively, are directed to a "Payment card (1), provided with a circuit (10)."

With respect to claim 24, the Examiner states:

> Bouricius et al. disclose a system which includes the secure transmission to a host machine of a transaction message which describes a financial transaction between a person and a retailer (column 3, lines 53-57), means for an encryption circuit to carryout the encryption processes (column 5, lines 37-39), an electronic funds transfer card (column 2, line 26) and a portable transaction terminal device (column 2, line 27).
>
> It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use identification data of a payment means to produce a diversified key in addition to using a circuit to carryout a cryptographic method, a payment card and a payment terminal in order to prevent eavesdroppers on the transmission line from obtaining any information which could later be used for fraudulent, illegal, or any other purposes as stated by Bouricius et al. (column 2, lines 812).

The Bouricius patent does not disclose the Applicants' claimed "[p]ayment card . . . with a circuit." This card is further described in the specification at page 12, line 40 to page 13, line 4 which states:

> The payment system schematically shown in FIG. 10 comprises an electronic payment means 1 and a payment station 2. The electronic payment means 1 is, e.g., a so-called smart card, i.e., a card provided with an integrated circuit for storing and processing payment data. The payment station 2 comprises a card reader 21 and a processor circuit 22. The processor circuit 22 may correspond to the circuit 10 of FIG. 9. (Emphasis added).

Applicants' "payment card . . . with a circuit" is not the same as Bouricius' cited "electronic fund transfer cards" or "portable transaction terminal devices." A smartcard, referred to in the specification, is a particular device that has an embedded integrated circuit. A device that is "smart" enough to hold its own data and applications and do its own processing. Smart cards are different from "dumb" cards that have magnetic strips or barcodes and rely more heavily on networks.

Since, neither the Bouricius patent nor the Miyano patent (as discussed above), taken alone or in combination, provide any teaching or suggestion of the use of a smart card, claims 24 and 29 can not be rendered obvious by the teachings of these references taken singularly or in any combination.

Conclusion

Thus, the Applicants submits that none of the claims, presently in the application, is anticipated under the provisions of 35 USC § 102 or obvious under the provisions of 35 USC § 103. Furthermore, the Applicants also submit that all of these claims now fully satisfy the requirements of 35 USC § 112.

Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

Respectfully submitted,

March 31, 2005

Peter L. Michaelson, Attorney
Customer No. 007265
Reg. No. 30,090
(732) 530-6671

MICHAELSON & ASSOCIATES
Counselors at Law
Parkway 109 Office Center
328 Newman Springs Road
P.O. Box 8489
Red Bank, New Jersey 07701